Risk-Informed Decision Making: Successes and Current Challenges

George E. Apostolakis
Massachusetts Institute of Technology
apostola@mit.edu

Presented at the

NASA Risk Management Conference 2005 (RMC VI)

Orlando, Florida

December 6, 2005

Technological Risk Assessment

- Probabilistic Risk Assessment (PRA) supports Risk Management by answering the following questions (Kaplan and Garrick):
  - ➢ What can go wrong? (accident sequences or scenarios)
  - ➢ How likely are these scenarios?
  - ➢ What are their consequences?

- The dominant accident sequences must be reported.

PRA Complements Traditional Methods

- **PRA analyzes the system as an integrated *socio-technical* system. Thousands of accident sequences are analyzed in contrast to the relatively small number of design-basis accidents considered in conventional analyses.**

- **Traditional conservative methods have turned out to be either non-conservative in some cases or overly conservative.**

- **Resources can be allocated rationally.**

The Nuclear Experience before and after PRA

- **Before**: Probabilities of accidents were not quantified.
- **After**: Some uncertainties are quantified.

- **Before**: The core damage frequency (CDF) was thought to be very low.
- **After**: CDF estimates higher than previously believed.

- **Before**: The accident consequences were thought to be disastrous.
- **After**: Accident consequences significantly smaller.

Lessons Learned

- Beliefs without a risk assessment can be wrong.

- Precautionary (defense-in-depth) measures are not always conservative – some important failure modes were missed.

- In some instances, unnecessary regulatory burden is imposed wasting valuable resources.

Common Misconceptions

- ***All PRA analysts care about is the bottom-line numbers.*** **Not true. It is the engineering insights that they care about. The lower the probabilities that are reported, the more suspicious these analysts become.**

- ***PRA results are not useful when they are highly uncertain.*** **These uncertainties exist independently of whether we do a PRA or not. Quantification contributes to the common understanding of the issues. It is a useful input to the allocation of research resources.**

Uncertainties

- Is the scenario list complete? **(incompleteness)**

- Are the models in the scenarios accepted as being reasonable? **(model uncertainty)**

- Are the epistemic pdf of the scenario frequencies representative of the current state of knowledge of the community? **(parameter uncertainty)**

Consequences of Uncertainties

- **Decision making must be risk-<u>informed</u>, not risk-<u>based</u>.**
- **Traditional safety methods have a role to play.**
- **Difficult to assess how much conservatism (defense-in-depth) is sufficient.**

How Are Current Decisions Made?

- **The traditional safety requirements are largely intact.**
- **Engineering insights from QRA inform the decision-making process.**
- **The three phases of progress:**
  - **1: Familiarization.**
  - **2: Use of "negative" results.**
  - **3: Use of all QRA insights.**

Risk-Informed Framework

Traditional "Deterministic" Approaches

- **Unquantified Probabilities**
- **Conservatism**
- **Can impose unnecessary burden**
- **Incomplete**

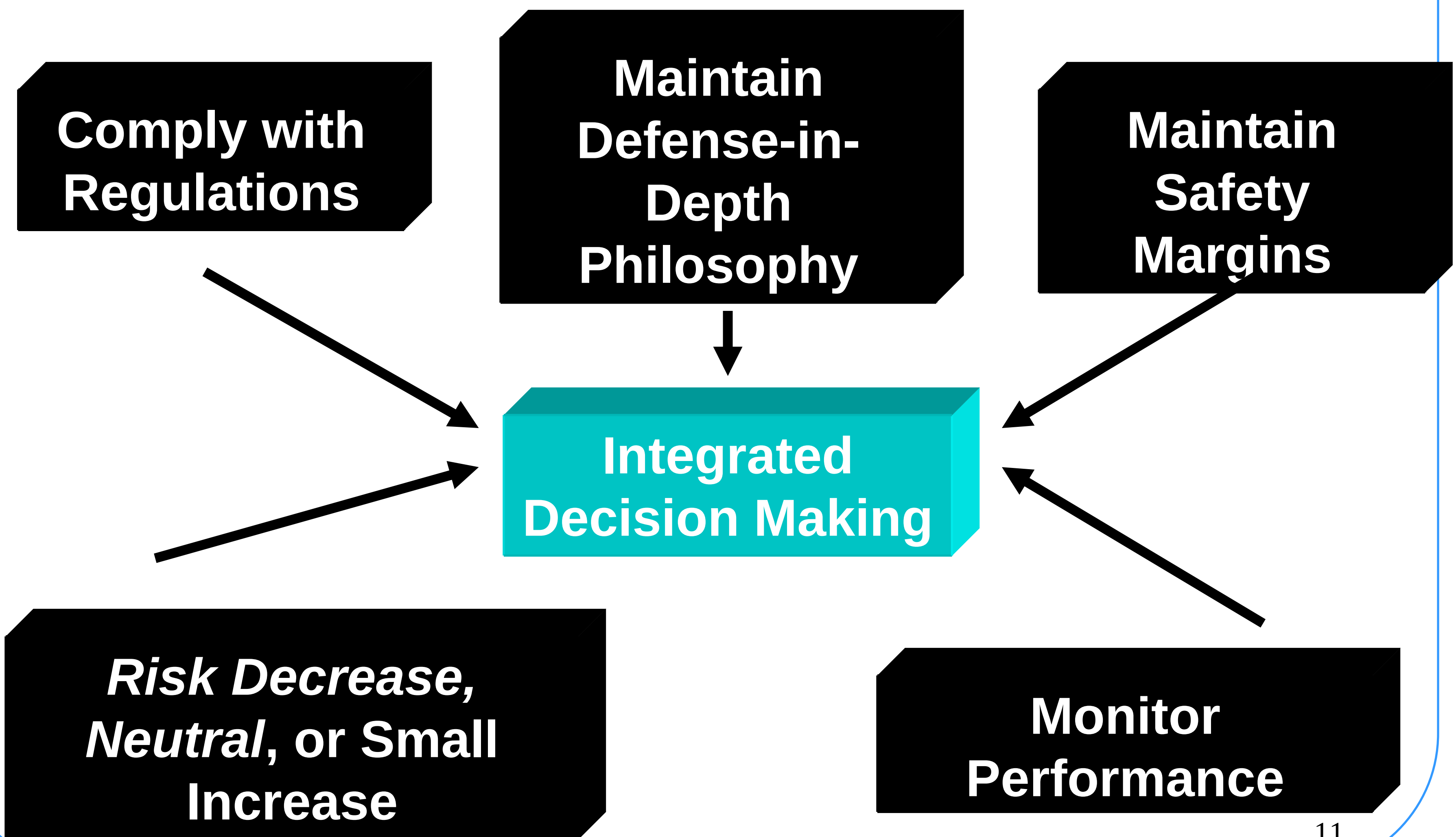
Risk-Informed Approach

- **Combination of traditional and risk-based approaches**

Risk-Based Approach

- **Quantified Probabilities**
- **Scenario Based**
- **Realistic**
- **Incomplete**

Risk-Informed Changes in the Licensing Basis



Successes and Challenges

- **Major Benefit: Prioritization of Systems, Structures, Components, and issues.**

- **Successes**
  - ➢ **Reactor Oversight Process**
  - ➢ **Management of Operations**
    - ✓ **In-Service Inspection**
    - ✓ **Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors.**

- **Challenges**
  - ➢ **Change in culture**
  - ➢ **Human error and digital software models**
  - ➢ **Risk-informing the regulations**

Current ASME Section XI Program

- **Inspect 25% of Class 1 Piping**
- **Inspect 7.5% of Class 2 Piping**

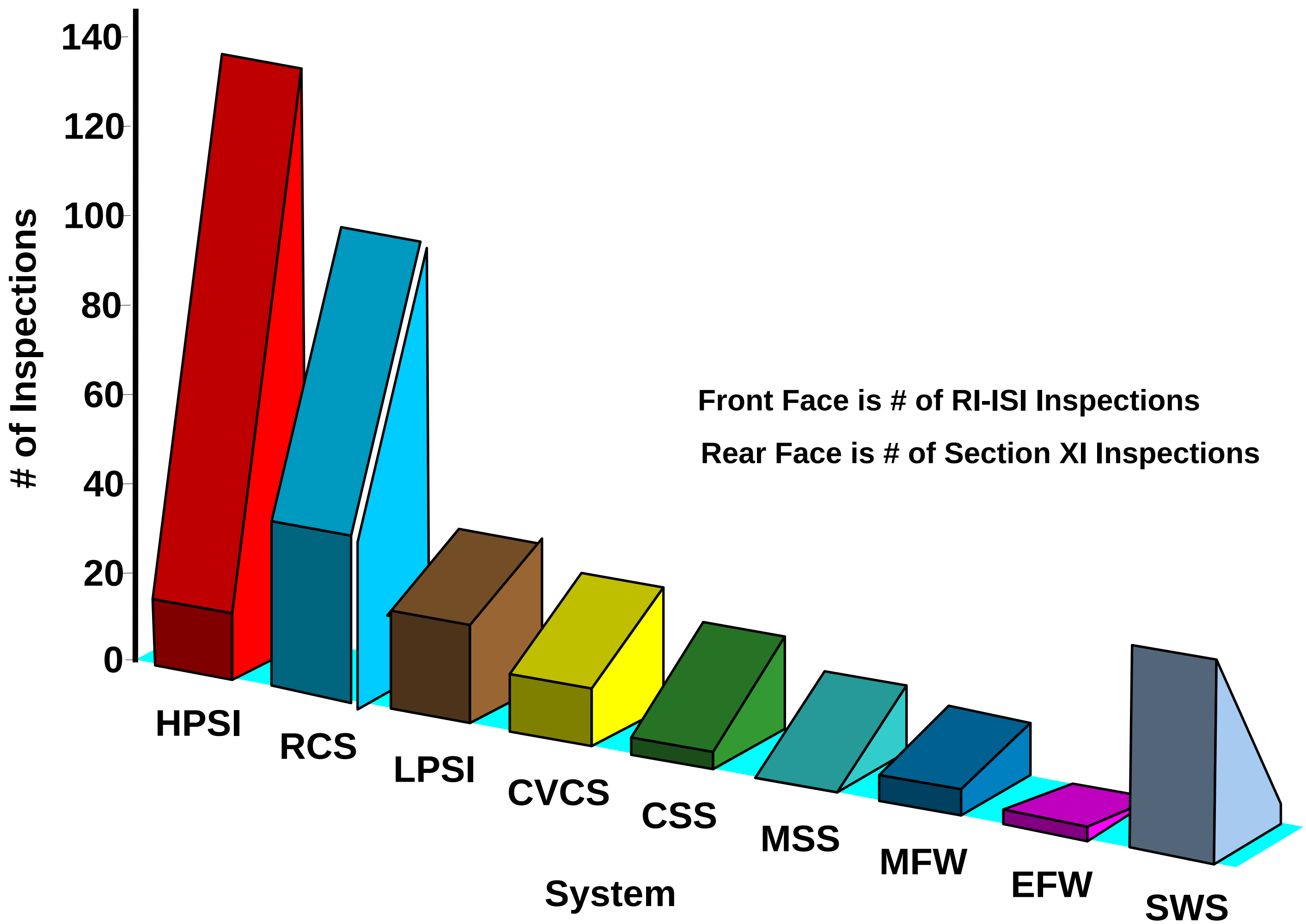
Selection based on the “stress level” or “fatigue usage”

Risk Matrix

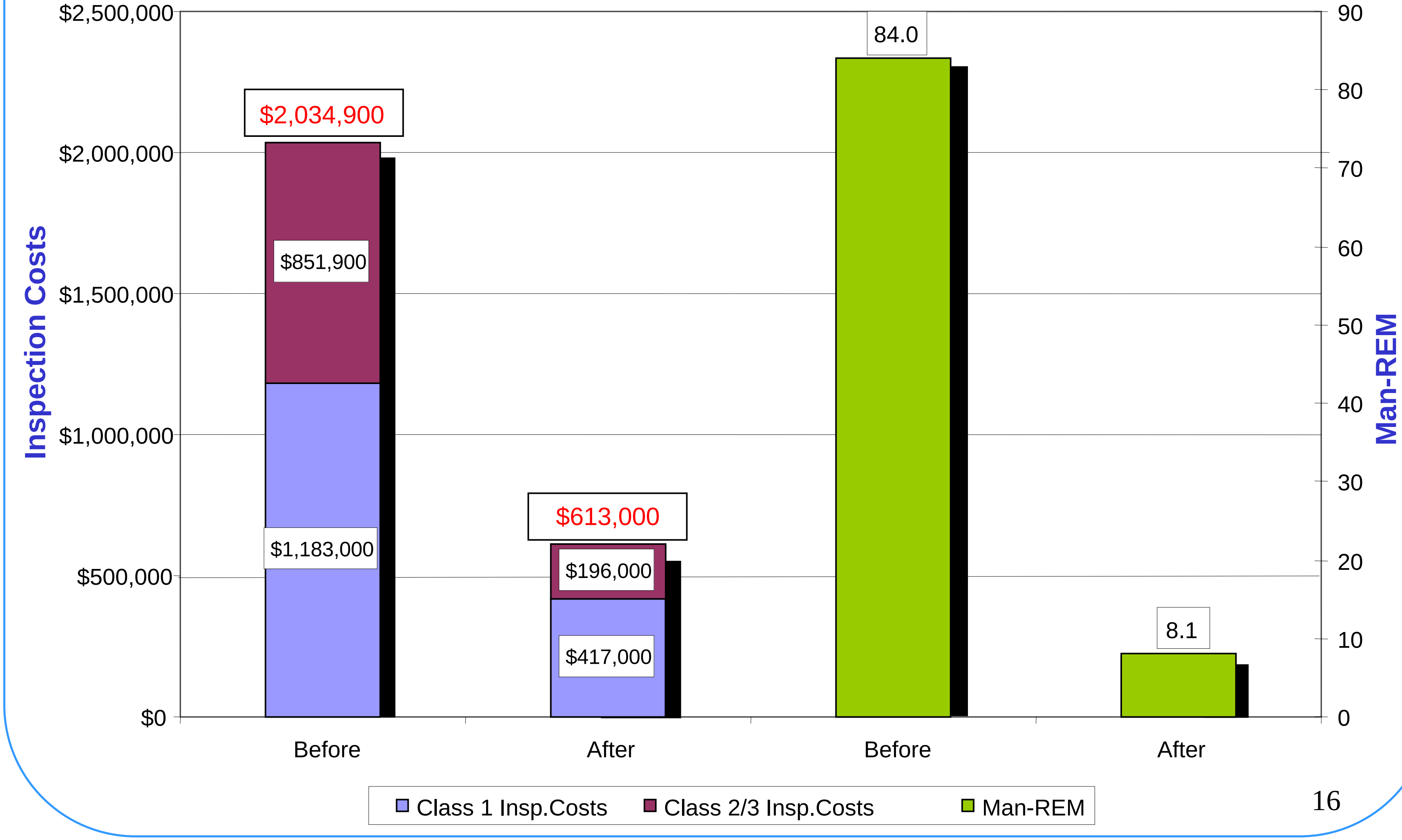
RELATIVE POTENTIAL FOR RUPTURE	Consequence Category			
	None	Low	Medium	High
High	CAT7	CAT5	CAT3	CAT1
Medium	CAT7	CAT6	CAT5	CAT2
Small	CAT7	CAT7	CAT6	CAT4

- Inspection Region 1 (High Risk)
- Inspection Region 2 (Medium Risk)
- Inspection Region 3 (Low Risk)

Number of Inspections Before and After the Use of Risk Information



RI-ISI Cost and Man-REM Savings



Challenges

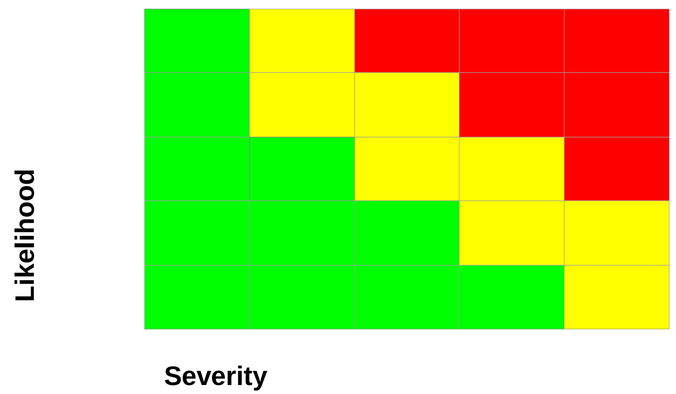
- **Dynamic Human Errors**
  - ➢ **Many models are available (e.g., ATHEANA, SPAR-H, ASEP, CREAM)**
  - ➢ **No consensus exists**
- **Safety Culture**
- **Digital Software**
  - ➢ **Different views: "software-centric" vs. "system-centric"**
  - ➢ **Failure modes may not be well understood**

A Preliminary Comparison

- **<u>Nuclear</u>:**
  - **Focus on safety (core damage frequency and large early release frequency).**
  - **Reliability and availability analyses decoupled from safety analyses.**
  - **Moving toward use of PRA as a design tool rather than just an assessment tool of existing reactors.**

- **<u>NASA</u>:**
  - **Focus of ISS and Shuttle PRAs on safety (Loss of Vehicle and Crew; Evacuation).**
  - **Primarily an assessment tool of existing systems.**
  - **Other objectives, e.g., mission success, handled separately.**

The Risk Matrix



- Applied to individual risk "issues."
- Total risk from all "issues" is not evaluated.
- Highly subjective; Uncertainties are not formally accounted for

A Broader Framework?

- Should we use formal methods (PRA) on safety issues only?
- Should we broaden the analysis to include additional objectives, e.g., mission success.
- If we do so, how should we make appropriate trade-offs?

The Value of Analytical Methods

- Two principal methods: Decision Theory and PRA.

- Each method provides:
  - "an organized, disciplined approach."
  - The rationale for the choices available to the Decision Maker (DM).
  - The ability to characterize the relevant uncertainties.
  - The ability to quantify the relative desirability of outcomes.
  - Rules for ranking the decision options, thus helping the DM to select the "best" one.
  - A systematic way to process large amounts of information.
  - A framework for enhanced communication.

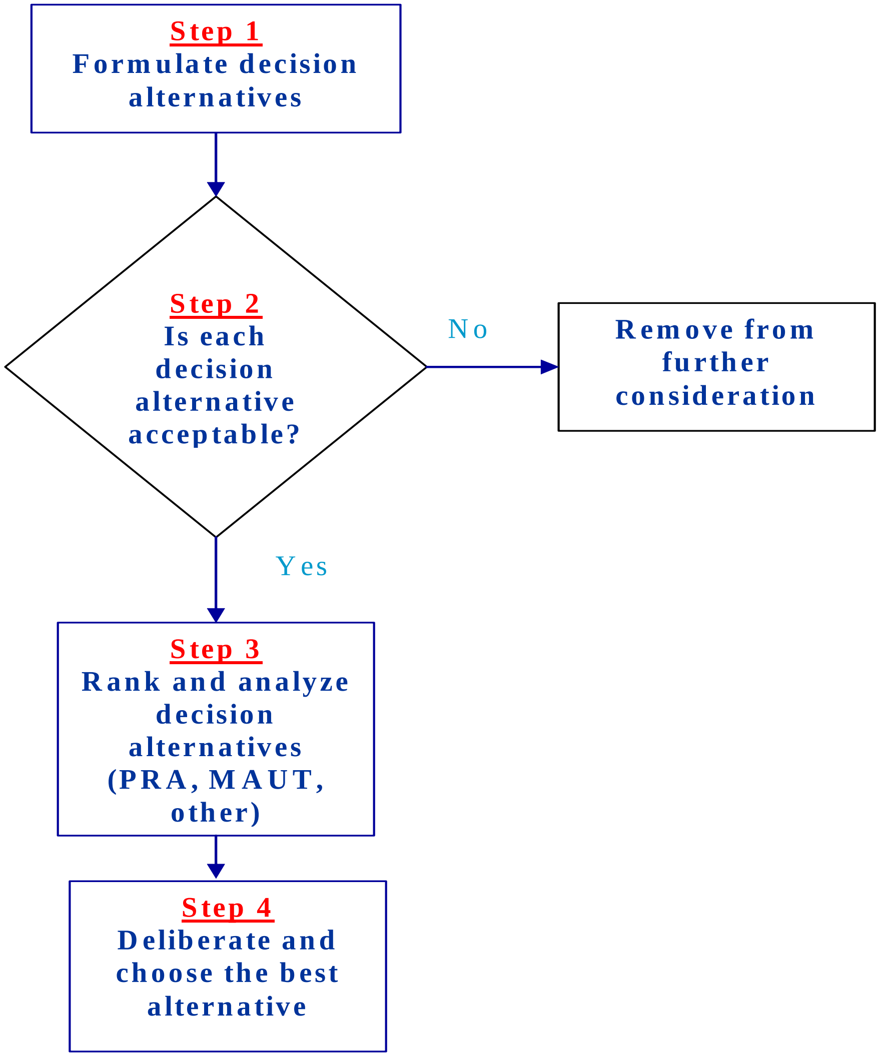
Why Risk-Informed Decision Making?

- **DA and PRA do not model everything of importance to the decision-maker.**

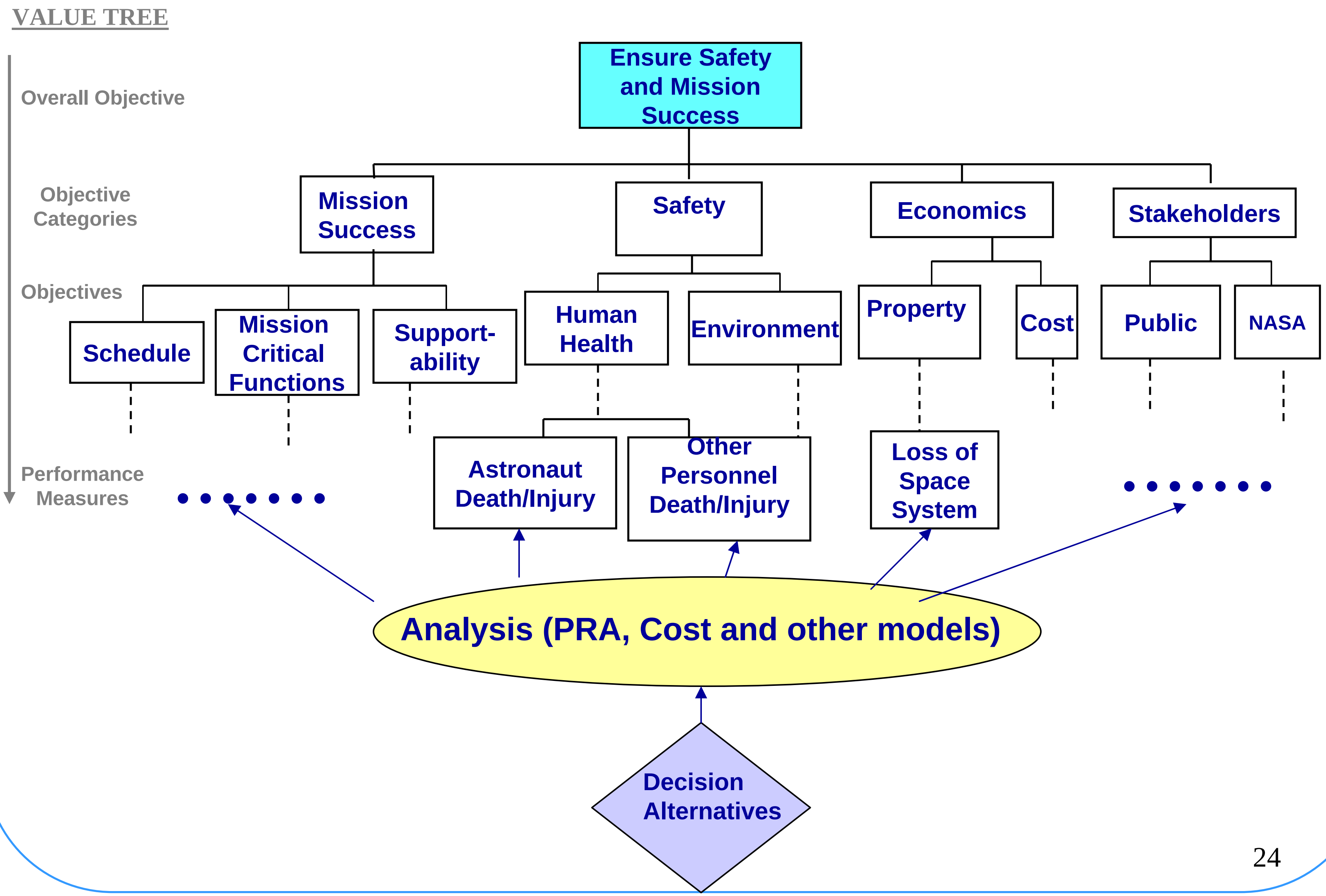
- **Analytic/Deliberative Process:**
  - ***Analysis*** **uses rigorous, replicable methods, evaluated under the agreed protocols of an expert community - such as those of disciplines in the natural, social, or decision sciences, as well as mathematics, logic, and law - to arrive at answers to factual questions.**
  - ***Deliberation*** **is any formal or informal process for communication and collective consideration of issues.**

National Research Council, *Understanding Risk*, 1996.

Analytic/Deliberative Decision Making



Overall View with a Preliminary Value Tree



References

Apostolakis, G.E., “How Useful is Quantitative Risk Assessment?’ *Risk Analysis*, 24:515-520, 2004.

Apostolakis, G.E. and Pickett, S.E., “Deliberation: Integrating Analytical Results into Environmental Decisions Involving Multiple Stakeholders,” *Risk Analysis*, 18:621-634, 1998.

Bley, D., Kaplan, S., Johnson, D., “The Strengths and Limitations of PSA: Where We Stand,” *Reliability Engineering and System Safety* 38: 3-26, (1992).

Kaplan, S. and Garrick, B.J., “On the Quantitative Definition of Risk,” *Risk Analysis*, 1 (1981) 11-28.

National Research Council, 1996, *Understanding Risk: Informing Decisions in a Democratic Society*. National Academy Press, Washington, D.C.

Pagani, L., Smith, C., and Apostolakis, G., “Making Decisions for Incident Management in Nuclear Power Plants Using Probabilistic Safety Assessment,” *Risk, Decision and Policy*, 9:271-295, 2004.

Sorensen, J.N., Apostolakis, G. E., Kress, T.S., and Powers, D.A., “On the Role of Defense in Depth in Risk-Informed Regulation,” *Proceedings of PSA ‘99, International Topical Meeting on Probabilistic Safety Assessment*, pp. 408-413, Washington, DC, August 22 - 26, 1999, American Nuclear Society, La Grange Park, Illinois.

U.S. Nuclear Regulatory Commission, “An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant-specific Changes to the Licensing Basis,” Regulatory Guide 1.174 (RG 1.174), Revision 1, Washington, DC, November 2002.